On vous suit !

Contrôle et surveillance électroniques au travail

Rapport d'Andrew Bibby
Illustration de Jane Shepherd

UNI/GS/06-2006/0035/FR

Marta travaillait pour une grande compagnie d'assurances multinationale. Son travail consistait à traiter des déclarations de sinistres pour cette multinationale, qui avait externalisé une partie de son travail administratif deux ans auparavant, pour le confier à une entreprise spécialisée qui employait du personnel intérimaire : pour être précis, disons que le véritable employeur de Marta était en fait une agence d'intérim.

Travaillant depuis près d'un an pour cette agence, Marta exécutait l'une de ses nombreuses missions depuis qu'elle avait quitté l'école à l'âge de 18 ans. Elle travaillait dans un immeuble de bureaux, situé dans une banale zone industrielle. Chaque jour, elle glissait sa carte dans le dispositif de contrôle placé à la réception et montait l'escalier pour rejoindre son bureau. Elle était censée travailler en équipe mais les visages autour d'elle changeaient sans arrêt. De toute façon, elle n'avait guère le loisir d'établir des contacts avec ces gens. En effet, les séries de déclarations de sinistre qu'elle devait traiter arrivaient automatiquement dans son ordinateur et sa tâche consistait à les traiter au fur et à mesure. Chaque sinistre devait en moyenne lui prendre six minutes et 42 secondes. L'ordinateur savait exactement à quel rythme elle allait et si elle n'atteignait pas l'objectif fixé à la fin de la semaine, son chef d'équipe la convoquerait pour un entretien.

Le travail était monotone, mais c'était tout de même du travail : attendant son premier enfant, elle avait besoin d'un salaire. Les cinq premiers mois de sa grossesse avaient été difficiles, mais elle avait lutté de façon à ne pas manquer un seul jour de travail, même si elle avait dû prendre des pauses plus souvent. Quoi qu'il en soit, elle était certaine d'avoir fait le maximum.

Mais tel n'était pas l'avis de l'entreprise. Un vendredi après-midi elle fut appelée au bureau du directeur. Devant lui s'amoncelaient des imprimés d'ordinateur. "Nous nous voyons contraints de vous renvoyer" a-t-il dit. "J'ai surveillé les pauses que vous avez prises. Regardez: là, par exemple, vous avez pris quatre pauses en une matinée la semaine dernière. C'est trop".

Les imprimés contenaient une ventilation détaillée minute par minute de tout ce qu'elle avait fait durant son travail au cours des dernières semaines, et notamment chacune de ses absences de son poste de travail. Marta fut très étonnée: "Je ne savais pas que j'étais ainsi surveillée" a-t-elle fini par dire. Son directeur a alors levé les yeux de ses papiers – "Vous ne le saviez pas ?" dit-il."Nous savons à tout moment où chaque personne se trouve dans le bâtiment. Votre badge de salarié comporte un dispositif de radiofréquence. Oh, à propos, vous devriez le laisser ici, vous n'en aurez plus besoin[1]".

Marta Redding n'est pas le vrai nom de cette salariée – mais l'incident est authentique.

Avant-propos

Personne n'aime avoir l'impression d'être espionné. L'idée que leur employeur pourrait les surveiller subrepticement laisse un goût amer aux travailleurs. Ce genre de pratiques n'est pas vraiment de nature à donner confiance – et pourtant, cette confiance est indispensable si l'on veut entretenir des relations du travail constructives.

Malheureusement, le présent rapport montre que les employeurs disposent à présent d'innombrables gadgets et autres bidules de haute technologie pour soumettre leur personnel à des niveaux élevés de contrôle et de surveillance électroniques.

Citons par exemple les minuscules étiquettes électroniques d'identification par radiofréquence (RFID), qui peuvent être utilisées pour suivre à la trace tous les individus à chaque minute de la journée, et qui peuvent être ajoutées au badge de salarié voire même cousues dans les uniformes de travail.

La RFID, de même que d'autres technologies de localisation, par exemple les systèmes de GPS basés sur le satellite, peuvent être utilisées dans des conditions telles que les salariés ne pourront jamais se sentir délivrés du travail même durant les pauses et durant leur temps libre.

Un autre exemple est celui des locaux munis de dispositifs de vidéosurveillance (qui sont aujourd'hui beaucoup plus précis car équipés d'un logiciel capable d'analyser les images numériques). On citera aussi la surveillance de la frappe sur le clavier de l'ordinateur, de même que le contrôle des appels téléphoniques, des courriers électroniques et toutes sortes d'autres pratiques qui font que les travailleurs se sentent constamment surveillés.

Loin de contribuer à développer le potentiel humain et à construire une "société de la connaissance", il semblerait que les technologies de l'information soient parfois utilisées pour empêcher l'individu de penser et agir de manière autonome au travail. En même temps, force est de constater que ces technologies mettent en péril le droit humain fondamental au respect et à la dignité au travail.

Bien entendu, les nouvelles technologies ne sont pas en soi un mal qu'il faudrait combattre. Le présent rapport a plutôt pour objet de mettre en relief certains des abus commis sur les lieux de travail, parfois tout simplement parce que les employeurs ont sélectionné sans réfléchir des options que leur offraient les logiciels.

UNI est déterminée à œuvrer pour éradiquer de tels abus, tout en s'efforçant d'encourager le développement des bonnes pratiques.

Philip J. Jennings
Secrétaire général d'UNI

Introduction

Depuis quelques années, on assiste à une explosion du contrôle et de la surveillance électroniques au travail, notamment avec l'apparition de nouveaux outils de technologie numérique très sophistiqués.

Ces technologies peuvent être utilisées à bon escient, de manière à faciliter la vie et la rendre plus conviviale tant pour les employeurs que pour les salariés. Mais le plus souvent, elles sont mises en place à des fins nettement moins sympathiques. Parfois, les employeurs utilisent ces outils sans réfléchir (‘c'est le logiciel qui est ainsi fait’); d'autres fois, cette initiative peut venir d'une croyance (généralement infondée) selon laquelle une main-d'oeuvre très surveillée serait plus productive. Il arrive aussi que certains exploitent cette possibilité pour rendre leurs salariés passifs et dociles de façon à les dissuader d'exercer leur droit à la syndicalisation et à la représentation collective.

Presque tous les secteurs d’UNI sont plus ou moins directement touchés par ces pratiques.

Le présent rapport examine par le détail sept moyens de contrôle et de surveillance électroniques au travail:

- L'identification par radiofréquence (RFID)
- Les ordinateurs "portés" et les technologies vocales
- La localisation par satellite et téléphone cellulaire
- La vidéosurveillance
- La surveillance du courrier électronique et de l'Internet; la surveillance de la frappe clavier
- La surveillance des appels téléphoniques et du travail dans les centres d'appel
- La surveillance biométrique et par implants

Le rapport analyse également certaines conséquences de la surveillance et du contrôle électroniques pour les syndicats, et examine en particulier l'impact de ces pratiques sur l'organisation et le recrutement, la santé et la sécurité, et la vie privée des travailleurs; il expose également un plan basé sur la notion de travail décent définie par l'Organisation internationale du Travail. Il s'achève par l'énoncé d'un certain nombre de suggestions concrètes en vue d'une action ultérieure d’UNI et de ses affiliés.

1. L'identification par radiofréquence (RFID)

L'identification par radiofréquence a vocation à devenir l'une des nouvelles technologies les plus envahissantes. Les étiquettes (ou "marqueurs") RFID sont déjà utilisées dans de multiples contextes, par exemple: les cartes à puce pour payer le bus, l'autoroute ou le métro dans de nombreux pays; les dispositifs de sécurité électronique fixés par les détaillants aux vêtements pour décourager le vol; les étiquettes à bagages dites "intelligentes" utilisées dans certains aéroports et même sous forme de puces de mesure électronique du temps pour les coureurs de marathon. Dans le commerce, les étiquettes RFID sont largement utilisées ainsi qu'en logistique pour la traçabilité et la gestion des stocks dans les entrepôts; ces étiquettes sont devenues obligatoires pour les fournisseurs de grandes enseignes telles que Wal-Mart.

Les étiquettes RFID sont des micropuces, parfois pas plus grosses qu'un grain de sable, qui contiennent des données spécifiques permettant d'identifier l'objet ainsi étiqueté. Munies d'une micro antenne, elles sont lues à distance par un lecteur RFID. Selon la radiofréquence utilisée et le type d'étiquettes, elles peuvent être lues dans un rayon allant jusqu'à plusieurs kilomètres. Mais le plus souvent, les étiquettes RFID sont destinées à être utilisées dans des circonstances qui n'exigent que des transmissions sur de courtes distances. Les étiquettes peuvent être passives (et sont "réveillées" au moment de la lecture) ou actives, et sont alors équipées de leur propre micro-pile et d'un transmetteur.

Le prix des étiquettes RFID les moins coûteuses est tombé en dessous de 50 cents des États-Unis, de sorte que l'utilisation de masse de cette technologie devient de plus en plus viable. Les détaillants prévoient que les étiquettes RFID remplaceront bientôt les codes-barres sur les rayons des supermarchés ; la grande différence est que les codes-barres sont génériques et renvoient à une ligne de produits donnés, tandis que l'étiquette RFID définit spécifiquement chaque article *individuel*. Des expériences pilotes ont été menées dans plusieurs pays.

Le recours au système RFID est controversé. Aux États-Unis, l'association CASPIAN – Consumers Against Supermarket Privacy Invasion and Numbering *("Les consommateurs contre les intrusions dans la vie privée et la détention de chiffres par les supermarchés"*) fait résolument campagne contre ce système. La CASPIAN affirme que les étiquettes RFID fournissent aux commerçants un mécanisme permettant de surveiller les comportements individuels des acheteurs, et que ces "puces espionnes" pourraient devenir un outil puissant d'intrusion dans la vie privée des personnes[2].

Les étiquettes RFID peuvent être utilisées pour identifier et surveiller les personnes autant que les objets. Elles sont déjà disponibles dans des pays tels que les États-Unis et le Japon pour surveiller les mouvements des personnes âgées dans les maisons de retraite, les patients et les personnels dans les hôpitaux, les nouveau-nés dans les maternités et les enfants dans les écoles. Dans ce dernier cas, l'utilisation de la RFID a également déclenché une polémique. Une école élémentaire près de Sacramento en Californie a récemment été obligée, sous la pression des parents, de cesser de suivre les enfants au moyen du système RFID[3].

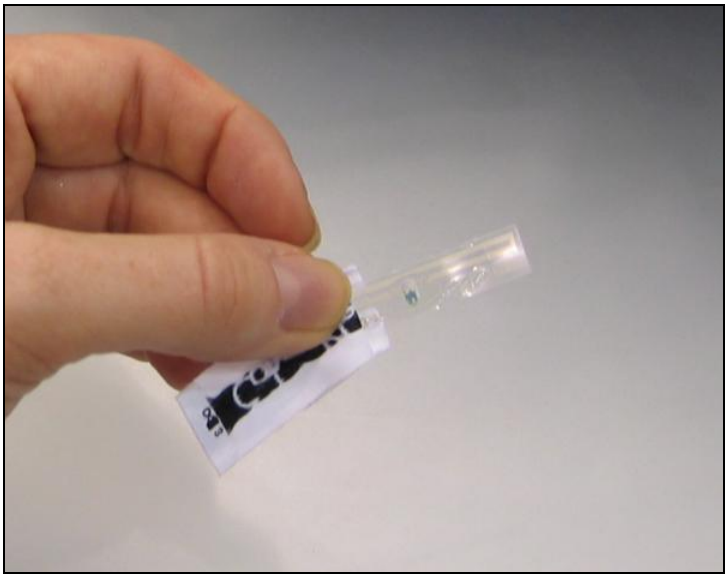
Dans le milieu de travail[4], les motifs de préoccupation concernant la RFID seront sans doute concentrés sur deux problèmes : tout d'abord, l'étiquetage RFID de biens et d'objets pourrait aboutir à une déqualification de certains emplois et à des contraintes de travail ayant pour effet d'assujettir les salariés à des impératifs techniques. Nous reviendrons plus loin sur ce point, dans le contexte du changement des pratiques de travail dans les entrepôts.

Mais il y a plus grave : la RFID offre la possibilité de surveiller les travailleurs tout au long de la journée de travail (et même au-delà). Cette pratique peut-être souhaitable dans certains cas précis, par exemple, peut-on lire dans un rapport, dans le cas des mineurs d'Afrique du Sud et du Chili, qui travaillent avec des appareils respiratoires munis d'une étiquette RFID permettant de les localiser en cas d'urgence[5]. Toutefois, de tels cas d'utilisation bénéfique risquent d'être l'exception plutôt que la règle.

Voyons par exemple ce compte-rendu sur l'utilisation de la RFID associée à d'autres formes de surveillance électronique, lancée par la société japonaise d'électronique Omron dans son usine de Kyoto :

“Le nouveau système d'Omron pour la gestion de la production fait appel aux étiquettes RFID, à des caméras vidéo, des systèmes de contrôle des accès et de la sécurité etc. afin de surveiller le niveau de productivité des salariés. Ceux-ci sont obligés de porter leur étiquette RFID afin que le système puisse surveiller leurs allées et venues de même que leur rendement. Les mesures précitées permettent d'optimiser l'attribution des primes aux salariés et d'améliorer la qualité des produits.[6]”

L'une des méthodes permettant de suivre les employés au moyen de la RFID consiste à coudre les étiquettes sur les uniformes. Les dispositifs peuvent être placés par exemple sur une étiquette de marque (la photo ci-dessous[7] montre l'envers d'une petite étiquette de Calvin Klein doublée d'une étiquette transparente de RFID); les concepteurs de RFID font également des essais dans lesquels les fibres des vêtements sont utilisées comme antennes de RFID. Les vêtements munis de ce dispositif peuvent être lavés normalement et sans dommage pour le marqueur RFID.



Par exemple, les serveuses d'un casino de Las Vegas portent maintenant des uniformes munis d'étiquettes RFID servant à surveiller leur travail. Selon l'un des cadres supérieurs de l'entreprise, le système aurait permis dès le premier jour de sanctionner une employée qui "flemmardait"[8].

Les personnels employés par les casinos du vaste complexe "Star City" de Sydney, Australie, portent également une étiquette RFID cousue sur leur uniforme.[9] Toutefois, il semblerait que cette mesure ne vise qu'à faciliter la gestion du vestiaire et (malgré les réticences initiales du personnel), elle a été jugée acceptable. Les salariés de Star City sont syndiqués par l'affilié d'UNI LHMU (Liquor, Hospitality and Miscellaneous Union). Le LHMU précise que les salariés ne portent pas l'uniforme à la maison et qu'ils ne sont donc pas surveillés en dehors de leur travail.

Pour autant, il n'est pas nécessaire de porter une étiquette RFID sur un uniforme pour être étroitement surveillé tout au long de la journée de travail. L'utilisation de loin la plus répandue des puces RFID au travail est celle des badges portant le nom de la personne ou des cartes d'identification pour le contrôle des entrées dans les immeubles et les locaux de travail.

Bien que de nos jours, les badges d'identité munis de RFID soient considérés comme une pratique normale sur de nombreux lieux de travail, ces badges procurent à l'employeur des données qui vont bien au-delà du contrôle des entrées. Le plus souvent, les données collectées sont reliées à d'autres bases de données de l'entreprise, notamment les RH et les registres de salaire. Une entreprise de TI propose par exemple des logiciels qui utilisent les données obtenues par les systèmes de contrôle d'entrée pour établir une série de rapports "notamment sur l'assiduité, les heures de présence, le salaire, les heures supplémentaires, un résumé de la feuille de paie, les absences, les appels nominaux, la liste du personnel, les départs avant l'heure …"[10].

La RAND Corporation a récemment conduit une enquête sur l'utilisation des données fournies par les badges munis de RFID dans six entreprises des Etats-Unis. Elle a constaté que les pratiques en vigueur intervenaient presque toujours à l'insu des salariés. Elle résume les résultats en ces termes:

"Les entreprises utilisent les cartes d'accès au site munies de systèmes RFID à bien d'autres fins que l'ouverture des portes (p.ex. pour faire appliquer les règles de bonne conduite au travail). En général, il n'existe aucun texte écrit et explicitement formulé au sujet de ces cartes, et rien n'est dit aux salariés quant aux politiques suivies. Le recours à ces systèmes a modifié l'équilibre traditionnel entre la convenance personnelle, la sûreté et la sécurité de l'entreprise, et le respect de la vie privée, d'où la perte de la possibilité d'anonymat. Ces systèmes posent également problème quant au principe et au sens de la notion "d'information authentique".[11]

Les chercheurs de RAND ont été surpris et troublés de constater l'absence de politiques ou d'informations écrites à l'intention des salariés au sujet de ces pratiques. Ils ont conclu leur étude par cette formule: "tout lecteur utilisant une carte d'accès munie d'une puce RFID devrait se sentir mal à l'aise à la lecture de ces résultats".

En 2003, la conférence internationale des commissaires responsables de la protection des données et de la vie privée[12] a tenu un débat initial sur les répercussions de la RFID. Le groupe de travail de l'UE sur la protection des données s'est également penché sur cette question[13]. Le groupe de travail recommande que la surveillance au moyen de la RFID respecte les principes de la protection des données, notamment l'obligation d'aviser préalablement les intéressés quant à la présence d'étiquettes RFID, et le maintien du droit de chacun d'accéder à ses données personnelles. Toutefois, il est évident que dans les deux cas, la formulation de politiques internationales claires n'en est encore qu'à ses débuts.

Les syndicats ont eux aussi commencé à s'intéresser à la surveillance par RFID.


En juillet 2005, le syndicat britannique GMB a critiqué le Groupe de travail de l'UE sur la protection des données en lui reprochant de ne pas avoir examiné les conséquences de la RFID sous l'angle de la surveillance du personnel et des atteintes à la vie privée, et a demandé que l'UE interdise "le marquage" des salariés au moyen de la technologie RFID. Le syndicat a déclaré que ce système portait atteinte au droit inaliénable des travailleurs à la vie privée.[14]


ver.di (Allemagne) propose d'utiliser une liste des questions à se poser (ci-dessous) en cas d'utilisation de la RFID sur le lieu de travail[15]:

- Les salariés reçoivent-ils dans des délais acceptables les informations nécessaires quant aux projets d'introduction de la RFID et leur mise en oeuvre?

- L'utilisation des radiofréquences, des scanners ou des portiques photoélectriques présente-t-elle un danger pour la santé ou des risques pour les travailleurs sur le lieu de travail?
- Quel est l'influence de ces technologies sur les habitudes de travail et comment modifient-elles concrètement les conditions et le milieu de travail?
- Si la technologie RFID est appliquée, quel sera son effet sur la rationalisation?
- Les salariés recevront-ils une formation suffisante à l'utilisation de la RFID?
- Quelles sont les données et en particulier les données à caractère personnel, qui seront stockées, et durant combien de temps ?
- Les données cumulées seront-elles utilisées pour contrôler le comportement et les prestations des salariés?
- Qui veillera à empêcher toute utilisation abusive des données?
- Comment les travailleurs peuvent-ils se défendre contre les abus?

UNI Commerce a adopté une déclaration sur l'introduction de la RFID, appelant à un dialogue social sérieux avec les entreprises pionnières dans l'usage de cette technologie[16].

2. Les ordinateurs "portés" et la technologie vocale

A présent, l'identification des produits par le système RFID et par le code-barres traditionnel est associée à de nouvelles formes de technologie vocale et à des ordinateurs "portés", notamment dans les entrepôts du commerce de détail, créant ainsi un environnement où les salariés sont de plus en plus transformés en automates.

Le syndicat britannique GMB a fait "la une" de la presse nationale et internationale au milieu de l'année 2005, lorsqu'il a alerté l'opinion quant aux conditions de travail dans certains entrepôts du Royaume-Uni, qu'il a comparés à des "sites d'élevage en batterie": "Le travailleur n'a rien d'autre à faire qu'à exécuter les ordres de l'ordinateur. Celui-ci calcule combien de temps il lui faudra pour aller d'un endroit de l'entrepôt à l'autre, la durée de ses pauses et le temps qu'il doit prendre pour aller aux toilettes. Aucun manquement à ces horaires ne saurait être toléré. En effet, avec les dispositifs régissant la logistique des transports de produits alimentaires vers les supermarchés et les magasins, les travailleurs sont là pour assister l'ordinateur et non plus l'inverse.[17]"

Le GMB cite l'exemple d'un entrepôt de 12 000 m2 au Pays de Galles, qui dessert 240 magasins. Les travailleurs chargés de collecter les produits destinés à la livraison sont équipés d'ordinateurs portables fixés sur le poignet et l'avant-bras et connectés à un scanner fixé sur l'index. Cet ordinateur, qui est fabriqué par Symbol, entreprise de TI spécialisée, pèse 320-350 grammes (voir illustration)[18].

Selon l'entreprise Symbol, “le terminal fixé sur le poignet reçoit les instructions concernant les stocks à prélever via le réseau local sans fil connecté au serveur de l'entreprise. Un chariot vide arrive dans la zone où se trouvent les

marchandises, l'agent utilise son scanner pour lire le code-barres et le terminal à écran LCD lui indique dans quelle allée il doit se rendre, à quel endroit il doit prendre les marchandises et quelles sont ces marchandises. Lorsque l'agent arrive au bon endroit, il commence par lire le code-barres installé au début et au bout de l'allée, pour vérifier qu'il se trouve bien dans la bonne allée. Puis il utilise son scanner pour lire le code-barres à l'endroit où se trouvent les marchandises pour vérifier que ce sont bien celles qu'il doit prélever. Il scanne alors chacun des produits qui sont ensuite disposés dans le chariot[19]." Autrement dit, pour citer les paroles du GMB "Les seules fonctions exécutées par la personne humaine sont celles qui correspondent aux octets restants n'ayant pas encore été automatisés".

Les ordinateurs portés entrent dans deux catégories principales - ceux qui sont portés sur le poignet et/ou l'index et ceux qui sont portés sur la tête ou à la ceinture. Ils sont souvent combinés avec la technologie vocale, de sorte que les travailleurs des entrepôts portent des casques d'écoute par lesquels ils reçoivent des instructions orales formulées par l'ordinateur lui indiquant les marchandises à prélever. Les systèmes de technologie vocale fonctionnent généralement avec des progiciels de gestion des commandes et de gestion des entrepôts, capables de synthétiser les données contenues dans ces systèmes pour les convertir en langage parlé[20].

Le GMB et le Professeur Michael Blakemore, universitaire britannique qui a conseillé le syndicat sur cette question, ont indiqué que cette technologie pourrait avoir certaines conséquences sur la santé et la sécurité. M. Blakemore affirme qu'en dépit des problèmes de lésions causées par gestes répétitifs (RSI) déjà constatés avec les techniques traditionnelles, il est rarement reconnu que ces nouveaux équipements pourraient eux aussi avoir des incidences sur la santé[21].

Les systèmes de prélèvement des marchandises dans les entrepôts ne se limitent pas à automatiser les processus de travail et fournissent aussi à l'employeur un précieux outil de surveillance des travailleurs. Blakemore cite le commentaire d'une de ces entreprises: "le système est également très intéressant du point de vue de l'encadrement, car il assure une traçabilité fantastique de tout ce que font les travailleurs individuels".

3. Surveillance par satellite et par téléphone mobile

Au-delà de la RFID, il existe d'autres technologies qui permettent d'identifier avec une précision remarquable l'endroit où se trouvent des objets ou des personnes.

Actuellement, la navigation par satellite repose sur le système américain du GPS (Global Positioning System). Le GPS utilise un réseau de satellites initialement créé à des fins militaires et toujours géré par le Pentagone. Chaque satellite transmet continuellement des données identifiant sa position. Les récepteurs de signaux GPS les analysent et en comparant les données transmises par quatre satellites ou plus, il est possible de repérer leur propre position avec une grande précision ainsi que leur altitude par rapport au niveau de la mer. (Au moins quatre satellites devraient être "perceptibles" pour chaque récepteur à un moment donné).

L'Union européenne s'attache à mettre au point son propre système de navigation par satellite, rival du GPS et portant le nom de Galileo; le premier satellite destiné au réseau Galileo a été lancé en décembre 2005.

La technologie du téléphone cellulaire (mobile/portable) offre également la possibilité de repérer les emplacements où se trouvent des personnes munies d'un téléphone mobile activé. Le repérage s'effectue par l'identification de la distance entre le combiné et le pylône de transmission le plus proche. La connexion entre ces deux équipements constitue les réseaux cellulaires sur lesquels repose la téléphonie mobile. Dans les zones urbaines en particulier, où les antennes de transmission sont très proches les unes des autres, il est possible de repérer le porteur d'un mobile avec un grande précision, en général dans une fourchette de 10 à 25 mètres. Les téléphones portables peuvent être repérés même lorsqu'il n'y a pas de conversation en cours.

Ces deux technologies convergent étant donné que les téléphones mobiles et les ordinateurs personnels sont de plus en plus conçus pour l'utilisation du GPS. Au Japon par exemple, 20 % des téléphones mobiles fonctionnent aussi comme récepteurs de signaux GPS[22].

Les services de localisation par GPS et par téléphone mobile sont déjà exploités commercialement, souvent à des fins de cartographie numérique. Le GPS est de plus en plus utilisé dans les systèmes de navigation installés à bord des automobiles par exemple. Les opérateurs de téléphonie mobile explorent les possibilités de "services de localisation" (par exemple pour indiquer aux utilisateurs de mobiles où se trouvent : l'établissement de restauration rapide le plus proche, les distributeurs de billets, voire même leurs amis et autres connaissances).

Sur le lieu de travail, comme dans le cas des autres technologies, la localisation par GPS et téléphone mobile peut être utilisée de manière constructive pour faciliter la vie des travailleurs, par exemple :

- Le suivi des fourgons blindés peut apporter un supplément de sécurité aux convoyeurs, qui sont exposés au risque d'attaques
- La géolocalisation peut contribuer à la sécurité des travailleurs mobiles; c'est notamment le cas pour ceux qui travaillent seuls dans des lieux isolés ou potentiellement dangereux, ou de nuit
- Ce suivi peut aussi aider à localiser les travailleurs mobiles ou les chauffeurs en cas d'intempéries

Malheureusement, les faits tendent à démontrer que les employeurs utilisent le repérage à des fins nettement moins bénéfiques. Prenons par exemple ce cas rapporté par l'Institut national pour les droits des travailleurs aux États-Unis:

Howard Boyle, président d'une société d'installation de gicleurs anti-incendie à Woodside dans l'Etat de New York, a donné des téléphones portables à ses salariés sans les informer que ces appareils étaient équipés de GPS. Ainsi, M. Boyle peut savoir où ils se trouvent à tout moment, y compris durant les pauses et même en dehors de leur travail. "Ils n'ont pas besoin de le savoir" a dit M. Boyle. "Je peux les appeler et leur dire : 'où êtes-vous maintenant?' tout en regardant mon écran et en sachant exactement où ils se trouvent"[23].

La surveillance continuelle peut exercer des pressions insidieuses sur les travailleurs, qui se sentent observés à tout moment de la journée. Aux États-Unis, un chauffeur dont le camion est équipé du GPS décrit en ces termes ce qu'il ressent :

"C'est un peu comme si 'Big Brother' me surveillait du coin de l'oeil.... je me sens mis à l'épreuve lorsque je fais la queue pour avoir un café et à ce moment-là je me dis "hé, on me regarde, je dois partir[24]."

Au Canada, le syndicat des travailleurs et travailleuses des Postes du Canada (STTP) a demandé à ses adhérents de surveiller très étroitement les initiatives de l'entreprise Postes Canada, qui envisage d'installer des ordinateurs avec GPS à bord de plusieurs centaines de véhicules de distribution. Ces dispositifs peuvent repérer via le GPS l'emplacement de chaque fourgonnette et de savoir si le moteur tourne, si le véhicule se déplace et à quelle vitesse, et si les portières sont fermées. Postes Canada a déclaré aux syndicats que cette initative avait pour but d'indiquer au personnel d'encadrement si les chauffeurs conduisent prudemment et respectent les consignes de sécurité (cela au moyen de "rapports d'exception" délivrés par l'ordinateur)[25].

Le STTP a rappelé à Postes Canada les dispositions de la convention collective en vigueur, pour avoir la garantie que cette surveillance ne sera pas utilisée à des fins disciplinaires.

 En effet, la clause de la convention collective conclue par le STTP avec Postes Canada sur la surveillance des salariés dispose que : "En aucun temps ces systèmes [de guet et d'observation] ne peuvent être utilisés comme moyen d'évaluer le rendement des employées et employés et ne peuvent servir à recueillir aucune preuve à l'appui de mesures disciplinaires, à moins que ces mesures disciplinaires résultent de la commission d'un acte criminel.[26]"

Les syndicats sont également intervenus dans d'autres pays pour freiner l'utilisation du GPS à des fins de surveillance. Aux États-Unis,le syndicat des Teamsters a négocié avec UPS afin que les données provenant de la surveillance par GPS ne soient pas utilisées à des fins d'évaluation des travailleurs ou de mesures disciplinaires[27]. Les "Teamsters" ont également contesté l'utilisation du GPS par d'autres entreprises de transport et de courrier de même que par les services de l'Etat.

Lorsque des systèmes de surveillance sont installés, il est particulièrement important que les travailleurs puissent eux-mêmes s'assurer que la surveillance s'arrête durant les pauses et à la fin de la journée de travail.

 Amicus (Royaume-Uni/Irlande) signale qu'il s'est opposé avec succès à l'installation d'un dispositif de surveillance sur les véhicules de l'entreprise en invoquant une atteinte à la vie privée et a obtenu pour les salariés le droit de désactiver le système[28].

Les services de géolocalisation, en particulier par GPS, se développent rapidement depuis quelques années, bien que pour l'instant, cette évolution technologique n'en soit qu'à ses débuts. L'enquête 2005 sur le contrôle et la surveillance électroniques effectuée par l'American Management Association auprès de 526 entreprises des États-Unis, fait ressortir que 8% d'entre elles utilisent les systèmes de localisation des véhicules par GPS ou GPS/cellulaire et 5% suivent les salariés munis de téléphones mobiles[29].

La mise au point de dispositifs adéquats de garanties et de bonnes pratiques pour protéger la vie privée des personnes en déplacement n'en est encore qu'à ses premiers stades[30]. Le conseiller juridique canadien David Canton a élaboré un guide à l'intention des employeurs, dans lequel sont énoncées quatre conditions à remplir si l'on veut instituer la localisation par GPS[31]:

- déterminer la nécessité
- établir une politique de protection de la vie privée
- prendre en considération les aspects moraux de la surveillance
- obtenir le consentement des intéressés

Il prévient que si le GPS peut accroître l'efficacité et la productivité, "il peut aussi saper le moral des salariés, les inciter à se rebeller et éventuellement, à intenter des actions en justice".

Quant au National Workrights Institute aux États-Unis, il évoque des préoccupations plus générales expliquant qu'il est nécessaire de laisser aux individus la possibilité de protéger leur "anonymat géographique" en particulier dans leur vie privée. Il souligne notamment que : "lorsqu'un salarié sait que son supérieur surveille ses faits et gestes quotidiens, il pourra réfléchir à deux fois avant de participer à certaines activités. Par exemple, si son chef est un Républicain notoire, il pourrait décider de ne pas se rendre au Congrès national des démocrates."[32]

4. Vidéosurveillance

Il y a des années que les syndicats se préoccupent de la surveillance pratiquée ouvertement ou secrètement à l'aide de caméras de vidéosurveillance sur les lieux de travail. Dès 1993 par exemple, le CWA (Communications Workers of America) avait attiré l'attention d'une commission du Sénat américain sur le cas d'une salariée qui s'était aperçue que son directeur avait installé une caméra dans les vestiaires. Les images filmées par la caméra ont été surveillées par des gardes de sécurité masculins qui observaient les travailleuses lorsqu'elles se changeaient pour revêtir leur uniforme.[33] D'autres cas similaires d'installation de caméras dans les toilettes ou les vestiaires ont également été signalés dans d'autres pays[34].

La vidéosurveillance reste un problème qui déclenche régulièrement des conflits au travail, en particulier lorsque des caméras sont installées sans consultation préalable ou sont utilisées à l'insu des travailleurs pour surveiller leur rendement, ou encore à des fins disciplinaires. Un exemple récent nous vient de la Deutsche Post, qui a installé des caméras de sécurité dans la salle principale de tri à Berlin, où travaillent 650 salariés. Le plan prévoyait que les caméras seraient activées jusqu'à 50 heures par semaine. Un tribunal fédéral du travail d'Allemagne a jugé cette mesure excessive[35].

Aujourd'hui, le recours aux caméras de surveillance pose des problèmes plus graves que par le passé et cela à plusieurs égards. À l'époque, les images filmées par les caméras étaient visionnées en temps réel ou enregistrées sur bandes magnétiques. De nos jours, les données provenant des caméras se présentent le plus souvent sous forme numérique et en tant que telles, peuvent être stockées indéfiniment en même temps que d'autres données numérisées. On peut par exemple imaginer que des données numériques recueillies par les caméras de surveillance visant des employés individuels soient recoupées avec d'autres données numériques relatives à ces personnes, par exemple des informations dans le domaine des RH ou des données issues de la surveillance des courriers électroniques ou des conversations téléphoniques, pour procurer à l'employeur un outil d'information intégré très puissant pour chaque individu.

Le Groupe de travail de l'Union européenne sur la protection des données a attiré l'attention sur les risques que pourrait susciter le développement d'applications capables "d'interpréter" des images vidéo, par exemple par l'identification des individus filmés au moyen de la reconnaissance faciale. Dans son rapport 2004 sur la vidéosurveillance, le Groupe de travail fait état de: "l'utilité d'une évaluation des tendances de l'évolution des techniques de vidéo-surveillance, afin d'éviter que le développement d'applications logicielles basées sur la reconnaissance du visage des personnes et sur l'étude et la prévision des comportements humains enregistrés dans les images n'entraîne un passage massif et inconsidéré à une surveillance du type dynamique-préventive, par

opposition à la forme la plus commune de surveillance statique, qui vise surtout à informer sur des événements spécifiques et leurs auteurs. Cette nouvelle forme de surveillance repose sur l'acquisition automatisée des traits du visage de personnes physiques et de leurs comportements "anormaux"; elle prévoit aussi la possibilité d'envoyer des signaux automatisés d'alarme et de demande d'intervention qui pourraient créer des risques de discrimination"[36].

Autrement dit, il devient très important de voir dans la vidéo-surveillance non pas une simple mesure de sécurité en soi, mais une source de données qui pourront servir à des recherches et des analyses exploitant pleinement le pouvoir des ordinateurs contemporains. Cette tendance est par exemple illustrée par le nouveau logiciel de la société Cisco Systems, dénommé AVVID (architecture pour la voix, la vidéo et les données) qui selon cette entreprise peut être utilisé par les banques non seulement pour la sécurité mais aussi à des fins de marketing et de relations clientèle afin d'accroître au maximum l'efficacité des agences[37].

Cette évolution nous montre qu'il est d'autant plus urgent d'oeuvrer en vue d'un contrôle adéquat de la vidéosurveillance. Le Groupe de travail de l'UE pour la protection des données souligne l'importance de certains principes fondamentaux en matière de protection des données, et notamment la modération ("proportionnalité") quant à l'usage qui est fait de la vidéosurveillance et l'information préalable des personnes qui en sont l'objet. Dans le contexte de la vie professionnelle, le Groupe de travail défend le principe de la protection "des droits, des libertés et de la dignité" des salariés. Il commente en ces termes la situation :

"Il est nécessaire que les systèmes de vidéo-surveillance ayant comme finalité directe le contrôle à distance de la qualité du travail et de la productivité, et qui comportent donc le traitement de données à caractère personnel dans ce contexte, soient de règle interdite …"

"L'expérience concernant l'application de la surveillance met en évidence la nécessité que des endroits réservés aux travailleurs et qui ne sont pas destinés à une activité de travail (toilettes, douches, vestiaires et zones de repos) ne soient pas soumis à surveillance ; que les images récoltées à des fins exclusives de défense de la propriété et de détection, prévention et répression d'infractions graves, ne soient pas utilisées pour contester aux travailleurs des infractions disciplinaires de moindre importance ; que le droit pour les travailleurs de s'opposer en utilisant les images enregistrées soit garanti. Des informations doivent être fournies aux salariés et à toute autre personne travaillant sur les lieux."

La surveillance menée à l'insu des intéressés est particulièrement préoccupante, ainsi qu'il ressort d'un exemple venant de Suède : le syndicat suédois des travailleurs des transports, affilié d'UNI, est actuellement en négociation avec Securitas, en vue d'encadrer cette pratique.

Il y a déjà un certain temps que les fourgons de Securitas sont équipés de caméras ; cependant, celles-ci ne commencent à filmer qu'en cas d'attaque du

fourgon ou d'ouverture des portes non autorisée, pratiques qui ont été acceptées par les syndicats. L'attaque à main armée d'un fourgon de Securitas sur la principale avenue au Sud de Stockholm en décembre 2005 démontre l'importance de mesures de sécurité appropriées. Toutefois, les personnels de Securitas ont vivement critiqué la pratique consistant à filmer secrètement à partir de véhicules banalisés.

Le syndicat suédois des travailleurs des transports pense que ces négociations avec l'entreprise déboucheront sur un accord applicable à l'ensemble des pays nordiques[38]. Entre-temps, l'affilié danois d'UNI, le DFF, a déjà conclu un accord avec Securitas, qui limite le nombre de cas justifiant la vidéosurveillance et prévoit une protection contre l'utilisation à des fins disciplinaires des séquences filmées. Les travailleurs doivent être informés de la surveillance au moment où ils sont embauchés.

De manière générale, il existe déjà plusieurs exemples de bonnes pratiques en matière de contrôle par vidéosurveillance et plusieurs pays ont adopté des lois à cet effet; en Nouvelles Galles du Sud, Australie, la loi de 1998 sur la vidéosurveillance au travail assure une protection aux travailleurs. Cette loi a été promulguée à l'issue d'une série de conflits du travail dans cet Etat. Récemment, la loi a été étendue à d'autres formes de surveillance électronique. En Autriche, l'employeur qui souhaite installer un système permanent de vidéosurveillance doit auparavant obtenir le consentement du comité d'entreprise.[39]

En Belgique, l'utilisation de caméras au travail fait l'objet d'une convention collective négociée entre les partenaires sociaux en 1998. Ce texte, qui s'étend à l'ensemble du secteur privé, a force de loi.

La Convention belge repose sur les principes de finalité et de proportionnalité. La surveillance permanente est strictement contrôlée et n'est autorisée que dans les cas où il s'agit de protéger la sécurité des travailleurs ou les biens de l'entreprise. La surveillance secrète par caméra est interdite, sauf lorsqu'il existe des indications probantes d'activités relevant du droit pénal. Les caméras ne peuvent être installées qu'après consultation des syndicats, et les travailleurs concernés doivent en être informés à l'avance. La finalité de la vidéo-surveillance doit être clairement définie[40].

5. Surveillance du courrier électronique et de l'Internet ; surveillance de la frappe clavier

La surveillance du courrier électronique et de l'Internet au travail est au coeur de nombreux débats depuis quelques années, en raison notamment des problèmes pratiques qui se sont posés dans de multiples établissements et ont fait l'objet d'un nombre croissant de mesures disciplinaires individuelles.

L'UNI (et auparavant la FIET) peuvent se flatter d'avoir très tôt pris des initiatives en ce domaine, en lançant dès 1998 une campagne intitulée "des droits en ligne pour les travailleurs en ligne". Le code de conduite d'UNI sur les droits en ligne au travail expose une série de bonnes pratiques qui ont été reprises par les syndicats et d'autres organisations.

Le code d'UNI définit quatre aspects interdépendants qui caractérisent l'utilisation du courrier électronique et de l'Internet – le droit des représentants des travailleurs d'accéder aux équipements électroniques, l'étendue de l'accès au courrier électronique et à l'Internet à des fins personnelles, les conditions d'autorisation de cet usage personnel et enfin, le contrôle et la surveillance de l'usage du courrier électronique et de l'Internet. Le présent rapport se limite à traiter le dernier de ces quatre aspects.

 Le Code de conduite d'UNI inclut, sous la rubrique "contrôle et surveillance des communications" le passage ci-après:

L'employeur s'engage à ce que l'utilisation de l'équipement électronique de l'entreprise par le salarié ne fasse pas l'objet d'une surveillance clandestine ou d'un contrôle.

Les communications ne feront l'objet d'une surveillance ou d'un contrôle que si ceux-ci sont autorisés par une convention collective, si l'employeur est légalement tenu de le faire ou s'il a des motifs raisonnables de croire qu'un salarié s'est rendu coupable d'un délit pénal ou d'une infraction disciplinaire grave. L'accès au dossier de contrôle et de surveillance d'un salarié en particulier n'est possible qu'en présence d'un représentant syndical ou d'un représentant désigné par le salarié.

Le code de pratique d'UNI s'appuie largement sur des principes déjà solidement établis dans le cadre des procédures de protection des données à caractère personnel des salariés, ainsi que sur les dispositions de protection de l'OIT et les instruments de garantie des droits de l'homme[41].

Un certain nombre d'affiliés d'UNI ont repris cette initiative à leur compte et ont bien souvent élaboré leurs propres lignes directrices et codes de bonnes pratiques. On citera notamment l'exemple du GPA (Autriche), du MSF (devenu

Amicus) (Royaume-Uni/Irlande), de la CFDT BETOR-PUB (France), et du FNV Bondgenoten (Pays-Bas)(voir ci-dessous).

Le protocole du FNV Bondgenoten sur la protection de la vie privée dans l'utilisation de l'Internet et du courrier électronique inclut la clause suivante :

L'employeur ne doit pas lire le contenu des messages électroniques, qu'ils soient de nature personnelle ou commerciale. Aucune donnée personnelle concernant le nombre de messages, les adresses de courrier électronique et autres données pertinentes ne saurait être enregistrée et/ou contrôlée. Cela ne préjuge pas du droit de l'employeur d'effectuer des vérifications occasionnelles en cas de nécessité contraignante dans l'intérêt de l'entreprise. Le comité d'entreprise doit être avisé de ces vérifications.[42].

En Allemagne, ver.di s'est associé à l'IG Metall et au DGB (confédération des syndicats allemands) pour créer un site Internet sur les droits en ligne : www.onlinerechte-fuer-beschaeftigte.de, et mener parallèlement une campagne sur ce même thème. Lancée en mars 2002 à Berlin à partir d'un café Internet, la campagne a été largement relayée par la presse. Le site Internet, qui est interactif, propose des informations sur la législation et un forum de discussion.[43]. Cette initiative a été suivie par une Déclaration en six points sur l'usage de l'Internet, de l'Intranet et du courrier électronique, adoptée par l'Exécutif du DGB en février 2004[44].

Ce feuillet d'information, publié dans le cadre de la campagne des syndicats allemands sur les droits en ligne, porte le message suivant: "j'envoie des lettres car mon chef lit mes courriers électroniques"

Des conventions collectives sur ce thème ont été conclues dans différents pays, notamment en Autriche, ainsi qu'au Danemark (accord entre le HL-Service et les employeurs du commerce du Danemark)[45]. La convention collective nationale la plus importante a été signée en Belgique entre les partenaires sociaux au mois d'avril 2002.


La convention collective belge[46] (qui a force de loi au niveau national) établit des limites à la surveillance de l'activité en ligne des salariés. Pour ce qui est de l'Internet, les employeurs peuvent collecter des données sur la durée des connexions en ligne mais sans identifier les sites visités par les personnes. Quant au courrier électronique, ils peuvent enregistrer le volume et le nombre de messages mais sans indication des auteurs et destinataires.

L'utilisation du courrier électronique et de l'Internet par les salariés a également retenu l'attention de l'Union européenne. Le Groupe de travail de l'UE sur la protection des données a énoncé des principes généraux applicables à la surveillance du e-mail et de l'Internet – principes qui sont résumés sous les rubriques suivantes : nécessité, finalité [but], transparence, légitimité, proportionnalité, précision et rétention des données, et sécurité[47]. Le document de la Commission européenne pour la deuxième phase de consultation des partenaires sociaux sur les données à caractère personnel des travailleurs propose également un cadre européen englobant la surveillance électronique[48] et incluant notamment les dispositions suivantes :

- La surveillance secrète ne devrait être autorisée que conformément aux garanties fixées par la législation nationale, ou si une activité criminelle ou un autre acte répréhensible peut raisonnablement être soupçonné
- L'évaluation des performances des travailleurs et la prise de décisions à leur égard ne devraient pas être fondées exclusivement sur des données à caractère personnel collectées dans le cadre d'une surveillance électronique
- L'employeur ne peut, en principe, accéder au courrier électronique à caractère privé et/ou à d'autres fichiers privés…

Toutefois, on aurait tort de penser que cette vague d'initiatives règle tous les problèmes liés à l'usage du courrier électronique et de l'Internet. Au Canada par exemple, une récente enquête universitaire fait ressortir la multitude des politiques mises en place, alors même que des conventions collectives ont été signées. Selon l'auteur de cette recherche, les accords les plus faibles énoncent explicitement que les syndicats doivent reconnaître le droit des employeurs d'utiliser toute forme de surveillance électronique où et quand ils le souhaitent[49].

Aux États-Unis également, la surveillance électronique est largement répandue. Selon la American Management Association (AMA), 76% des employeurs surveillent les connexions Internet de leurs salariés et 55% enregistrent et lisent leurs courriers électroniques. L'enquête 2005 de l'AMA constate que plus d'une

entreprise sur quatre a licencié des salariés sur une allégation d'usage abusif de l'Internet et que 25 % des employeurs ont licencié du personnel pour usage abusif du courrier électronique. De plus, l'AMA a constaté qu'une entreprise sur dix surveillait l'usage de l'Internet par les salariés sans les en aviser et que 14% n'informaient pas le personnel que le courrier électronique était surveillé[50].

Il est difficile de ne pas partager l'avis d'Hubert Bouchet, de la Commission française informatique et libertés (CNIL), qui a attiré l'attention sur le fait qu'une large majorité de salariés ignorent qu'ils sont surveillés par l'employeur. "L'équilibre nécessaire entre contrôle légitime exercé par l'entreprise et respect des droits des salariés ne paraît pas assuré dans bien des cas."[51].

Il n'est pas sans intérêt de souligner que l'enquête menée sur le contrôle et la surveillance par l'American Management Association constate également qu'un employeur sur 3 (36%) contrôle le nombre de frappes clavier, le temps passé au clavier et/ou le contenu des textes saisis. Il y a déjà des années que les syndicats s'inquiètent des cas de dépression chez les travailleurs en raison de la surveillance permanente du clavier. L'exigence d'un niveau de productivité extraordinairement élevé dans le travail de frappe peut contribuer à l'apparition de lésions par gestes répétitifs, un phénomène qui atteint des proportions quasi épidémiques dans certains pays.

Gerrit Wiegand a effectué, pour le compte des syndicats allemands, une étude détaillée sur les applications de logiciels et matériels susceptibles d'être installés sur l'ordinateur pour surveiller la frappe clavier. Il rend compte de ses constatations dans l'ouvrage intitulé "Im Netz@work"[52].

Dans le commerce de détail, il y a longtemps que l'on exprime des préoccupations comparables à propos de la surveillance automatique du rendement des employés de caisse, qui est mesuré au nombre d'objets passés à la lecture optique, depuis la mise en service des caisses électroniques et des codes-barres. La technologie peut être utilisée pour surveiller avec précision tous les détails de la journée de travail des salariés, y compris la durée exacte passée aux toilettes. Toutefois, ce n'est pas parce que la technologie autorise cette forme d'espionnage électronique qu'il faut nécessairement s'en servir. On notera que dans le futur magasin de Metro à Rheinberg, les salariés ont la possibilité d'accéder à l'ordinateur de manière anonyme par exemple pour actionner les balances électroniques, de sorte qu'il ne sera pas procédé à la collecte de données à caractère personnel.

6. Surveillance des appels téléphoniques et travail dans les centres d'appel

Il existe plusieurs manières de surveiller les appels téléphoniques. On peut notamment enregistrer le nombre et la durée des appels ainsi que les numéros qui sont appelés; les conversations dans le cadre de ces appels téléphoniques peuvent être écoutées par le personnel d'encadrement, ouvertement ou subrepticement; les appels peuvent être enregistrés; quant à la messagerie vocale, elle peut aussi être surveillée et enregistrée.

Aux États-Unis, près de la moitié des entreprises américaines surveille les appels téléphoniques en enregistrant les numéros appelés et la durée des appels; les deux-tiers de ces entreprises effectuent cette surveillance à intervalles réguliers ou de manière permanente. Toutefois, selon l'American Management Association, 22% d'entre elles n'informent pas le personnel de cette surveillance. Près d'une entreprise sur quatre enregistre les appels[53].

Dans certains secteurs (par exemple la bancassurance) l'enregistrement des appels téléphoniques peut se justifier par des raisons légales ou réglementaires. Toutefois, cela ne veut pas dire que les appels enregistrés doivent nécessairement être utilisés à d'autres fins, par exemple pour surveiller la productivité des salariés individuels ou à des fins disciplinaires. Les appels téléphoniques sont de plus en plus stockés sous forme numérique ; là encore, à l'instar des enregistrements effectués par des caméras de surveillance, il est possible de recouper les données avec d'autres ensembles de données sur le personnel et de les analyser très minutieusement à l'aide de logiciels informatiques.

Les salariés devraient être avisés que leurs appels sont enregistrés.

Certaines entreprises affirment qu'elles écoutent ou enregistrent les appels à des fins de "formation". Si cette démarche peut être légitime dans certaines circonstances pour permettre aux entreprises de maintenir les niveaux de compétences, les personnes qui ont besoin d'une aide en ce domaine devraient pouvoir accéder à une formation adéquate. Là encore, les employeurs ne devraient pas utiliser cette forme de surveillance de manière abusive et à des fins autres que le but initial.

Les travailleurs employés dans les centres d'appels sont plus que les autres touchés par ces problèmes. Ainsi que le soulignait un rapport d'UNI sur le travail dans les centres d'appels, "De manière générale, la technologie des centres d'appels confère aux employeurs le pouvoir de maintenir des niveaux inouïs de surveillance et de contrôle électroniques de leur personnel"[54].

De plus, les travailleurs des centres d'appels n'ont que très peu d'influence sur le déroulement de leur journée de travail – ils prennent les appels qui sont automatiquement dirigés vers leur poste à l'aide de la technique de distribution automatique des appels (DAA), sont bien souvent obligés d'utiliser des formules toutes prêtes (scripts) lorsqu'ils parlent aux appelants, et doivent se conformer à des objectifs très stricts de vente ou de rendement. Le plus souvent, la technologie de DAA permet d'enregistrer tous les aspects des appels traités, y compris le temps passé en pause ou aux toilettes. Un récent bulletin d'information d'UNI sur les centres d'appels internationaux expose le cas d'une femme qui a été obligée de dire à son chef qu'elle était enceinte avant même d'avoir pu en informer sa famille, pour expliquer pourquoi elle se rendait "trop souvent" aux toilettes.[55] (c'est de cette affaire que s'inspire notre récit sur 'Marta', en première page du présent rapport).

La Charte et le Plan d'action d'UNI sur les centres d'appel, élaborés à l'occasion de la 1e Conférence d'UNI sur les centres d'appels en octobre 2005, traitent tous deux du problème du contrôle et de la surveillance.

 La Charte d'UNI sur les centres d'appel inclut six points sous la rubrique Surveillance, observation électronique et vie privée

- La surveillance ne peut être autorisée que lorsque son objectif est connu et acceptable
- Les données collectées ne peuvent être utilisées que dans ledit objectif
- L'employé doit savoir qu'il/elle est – ou peut être - surveillé(e)
- Les écoutes ne peuvent être qu'occasionnelles et en aucun cas continuelles
- L'employé doit avoir accès aux données enregistrées et être en mesure de corriger les erreurs
- Les enregistrements doivent être détruits après une certaine période

UNI Telecom a récemment lancé une autre initiative concrète dans le cadre du dialogue social européen avec l'association d'employeurs ETNO, en vue d'inclure une clause sur la surveillance dans les "Lignes directrices pour les centres de contact clients" précédemment adoptées. Cette clause repose sur le principe fondamental selon lequel les travailleurs de ces centres doivent être avisés de tout dispositif en vigueur quant à la surveillance du rendement.

L'expérience des affiliés d'UNI démontre qu'il est possible de négocier de meilleures conditions de travail pour les personnels des centres d'appels. Par exemple, plusieurs syndicats du secteur des télécoms ont négocié des conventions collectives incluant des dispositions sur les mesures de contrôle et de surveillance.

 Aux États-Unis, le CWA (Communications Workers of America) a négocié des accords avec un certain nombre d'entreprises de télécoms, dont AT&T, Qwest, Bell South et SBC[56].

L'accord passé avec AT&T limite la surveillance des appels :

- Les salariés seront préalablement avisés du jour où seront effectuées des écoutes par échantillonnage et chacun pourra choisir entre la surveillance à distance ou la surveillance avec présence physique
- Les écoutes individuelles seront effectués sur le lieu de travail de l'employé
- Aucun salarié ne fera l'objet de sanctions disciplinaires à l'issue d'un contrôle individuel de ses prestations, sauf en cas de faute de grossière à l'égard d'un client, de fraude, de divulgation abusive du contenu des communications, ou lorsque le salarié ne parvient pas à améliorer ses prestations.

L'accord conclu avec Pacific Bell (SBC) limite la surveillance du personnel à dix appels par mois.

En Australie, le syndicat CEPU (Communication Electrical and Plumbing Union) a également entrepris de lutter contre la surveillance excessive dans les centres d'appels. Les syndicats font pression sur les gouvernements des Etats d'Australie afin qu'ils acceptent de s'engager sur des normes minimales de travail dans les centres appel.

Le contrôle et la surveillance posent un grave problème dans les centres d'appels, car de nombreuses études attestent qu'il s'agit là d'un facteur de stress majeur pour les travailleurs. Ainsi qu'il ressort d'un rapport établi par une université britannique "Incontestablement, de nombreux travailleurs considèrent que les mécanismes de surveillance et de contrôle ajoutent encore aux tensions du travail. Ils sont plus d'un tiers à penser que l'enregistrement de leurs appels contribue "fortement" ou "dans une certaine mesure" aux pressions inhérentes à leur travail.[57]" Nous reviendrons sur ce point dans les pages qui suivent.

7. Surveillance biométrique et par implants

Ce dernier chapitre examine brièvement les perspectives de surveillance électronique des travailleurs par des méthodes plus directes et plus invasives – qui s'appliquent au corps humain.

La technologie de la biométrie (la reconnaissance des personnes basée exclusivement sur leurs traits physiques) est déjà utilisée dans de nombreuses situations de la vie quotidienne. La saisie des empreintes digitales par scanner a été instaurée aux États-Unis pour le contrôle des voyageurs étrangers arrivant dans le pays. La reconnaissance de l'iris de l'oeil est considérée comme une voie particulièrement prometteuse pour l'identification des personnes.

Les données biométriques, par exemple les empreintes digitales, se différencient de la méthode classique par le fait qu'elles sont numériques, alors qu'autrefois, la police prenait les empreintes digitales de suspects à l'aide d'un tampon d'encre et de papier. La nouvelle méthode permet de conserver les données enregistrées sous forme numérique et par conséquent, de les analyser de manière détaillée à l'aide de logiciels informatiques. La biométrie pourrait avoir des incidences graves sur la protection de la vie privée. Les syndicats devront surveiller très étroitement les initiatives visant à établir cette technologie sur le lieu de travail.

Le système biométrique est déjà utilisé dans la pratique, par exemple chez McDonalds, qui aurait instauré selon nos informations un système de saisie des empreintes du pouce et de la main dans certains de ses établissements au Canada[58]. Toujours dans ce pays, le syndicat des travailleurs et travailleuses des postes STTP a contesté les démarches entreprises par Postes Canada en vue de saisir numériquement les empreintes digitales de certains facteurs à des fins de "contrôle de fiabilité" [59].

Les fabricants d'étiquettes RFID ont fait un pas de plus en développant un système d'implantation de minuscules étiquettes RFID sous la peau des individus. Il serait rassurant de pouvoir dire que pour l'instant cette idée ne relève que de la science-fiction, mais malheureusement, tel n'est pas le cas. En effet, la société américaine Applied Digital fabrique déjà ce produit, dénommé "le VeriChip".

Le VeriChip est principalement commercialisé comme moyen de stockage d'informations médicales chez certaines personnes. Il a aussi été utilisé par une boîte de nuit, qui encourageait ses habitués à se faire implanter un VeriChip pour faciliter l'entrée dans l'établissement et le paiement des boissons. Ces puces sous-cutanées ont également été utilisées dans le contexte du travail, et plus précisément par dix-huit fonctionnaires volontaires employés par le parquet du Procureur général du Mexique. Ces puces (voir photo ci-dessous[60]) sont utilisées pour faciliter l'admission du personnel dans les zones d'accès restreint.

Les risques d'atteinte à la santé que présente l'implantation d'une puce RFID sont examinés ci-dessous. Mais avant même de songer à d'éventuels problèmes médicaux, il est bien évident que les nouveaux produits tels que le VeriChip peuvent avoir des répercussions majeures sur le droit à la vie privée au travail et en dehors.

Questions soulevées par la surveillance et le contrôle électroniques

Pourquoi cette évolution? Pourquoi un système de commandement et de contrôle assisté par électronique semble-t-il prendre le pas sur l'exigence de "travail intelligent" et de formes plus coopératives de participation des salariés, généralement préconisée par les RH en cette ère de l'information?

Pour répondre cyniquement, on pourrait dire que c'est parce que la technologie existe, tout simplement. Le Prof. Michael Blakemore, qui a conseillé le syndicat britannique GMB, commente ainsi le message "rassurant" que semble offrir ce type de technologie: "derrière ce discours se cache la promesse de sécurité, de sûreté et de bénéfices" écrit-il [61]. Mais il souligne aussi que le recours à cette technologie peut avoir de profondes répercussions au travail : "Il en résulte un changement de la relation entre la direction et le personnel - celle-ci n'engage plus la conversation avec les salariés et se contente de les surveiller"..

Cet auteur, de même que d'autres chercheurs, insistent de plus en plus sur la notion "d'invasion informatique" décrivant un processsus dans lequel les ordinateurs sont tellement incrustés dans la vie quotidienne qu'ils en deviennent invisibles et totalement banalisés[62]. Par analogie, la surveillance envahissante renvoie à une situation où, (pour citer encore Blakemore) "les moindres faits et gestes du salarié peuvent être surveillés, analysés et vérifiés".

Ainsi que l'OIT l'a souligné dans son rapport majeur de 1993 sur les conditions de travail, au chapitre de la surveillance, certains travailleurs sont plus visés que d'autres par ce phénomène : les formes de travail qui se prêtent le plus à une surveillance intensive sous souvent celles qu'exercent les femmes, les membres des minorités et de manière générale, les personnes faiblement rémunérées.[63] A cet égard, il est intéressant de noter que dans sa campagne contre les conditions de travail dans les entrepôts britanniques, qui sont comparés à des sites "d'élevage en batterie" (voir ci-dessus) le GMB souligne que ces établissements emploient une majorité de travailleurs migrants.

On peut donc en déduire qu'à l'ère de l'information, si certains travailleurs hautement qualifiés effectuent un travail à forte valeur ajoutée et sont libérés des contraintes de la surveillance hiérarchique, beaucoup d'autres risquent d'être enchaînés par la technologie – dans un contexte qui ressemblera fort à ce que l'on appelait autrefois "le travail à la chaîne".

La surveillance électronique est peut-être une pratique "rassurante" pour les entreprises, mais est-elle au moins efficace ? Il semblerait que très souvent, ce ne soit pas le cas. Dans un ouvrage datant de 1999, Gary Marx, du MIT, affirme que: "à présent, les partisans de la surveillance électronique n'ont pas beaucoup d'arguments solides pour étayer leurs théories. Nous verrons probablement par la suite que la surveillance tous azimuts risque, à juste titre, de s'avérer contre-productive. Les atteintes à la santé physique et mentale des travailleurs pourraient annuler les avantages d'une hypothétique amélioration de la productivité obtenue par cette surveillance. [64]“

Mais la question n'est pas de savoir si cette surveillance est ou non "efficace" pour les entreprises. Quoi qu'il en soit, même si l'on avait des preuves que la surveillance totale des travailleurs apporte des avantages à l'entreprise, les syndicats ont de bonnes raisons de s'opposer à cette pratique. Trois d'entre elles sont analysées ci-dessous.

Le droit à la représentation collective

Voici tout d'abord un premier argument qui relève du bon sens: les syndicats peuvent craindre avec raison que le contrôle et la surveillance ne soient utilisés par des employeurs hostiles comme outil de dissuasion pour étouffer la représentation collective.

Plusieurs cas concrets confirment que la surveillance a été instaurée au moment où les syndicats s'efforçaient d'organiser les non-syndiqués. L'exemple de Wal-Mart est édifiant: cette entreprise qui est notoirement la plus hostile de toutes au syndicalisme a installé des caméras de surveillance dans un de ses magasins du Kentucky au moment où l'UFCW tentait d'organiser le personnel. Il semblerait qu'elle ait récidivé en Indiana et probablement dans d'autres régions des Etats-Unis.[65]

Même dans les établissements où les syndicats sont reconnus, la surveillance étroite infligée aux travailleurs toute la journée n'est pas de nature propice à un travail syndical efficace. Ainsi que le souligne Eric Lee, autrefois les travailleurs pouvaient plus facilement communiquer leurs problèmes aux représenants syndicaux, par exemple en chuchotant à côté d'un rafraîchisseur d'eau[66]. Plus la journée de travail est surveillée, moins les travailleurs ont de chances de communiquer de manière informelle avec leurs représentants.

Questions de santé et de sécurité

Les nouvelles technologies engendrent de nouveaux risques pour la santé et la sécurité. Lorsque la saisie des données sur clavier d'ordinateur est devenue une activité à part entière, on a constaté une augmentation généralisée du nombre de personnes souffrant de lésions causées par gestes répétitifs, de même que dans les centres d'appels, les travailleurs sont menacés par le danger de choc acoustique.

Il n'est pas toujours facile de définir exactement les risques de "l'invasion informatique" pour la santé des travailleurs. Dans les notices techniques, les fabricants des technologies décrites dans le présent rapport ne disent pas grand chose sur les questions d'ergonomie ou de santé et de sécurité au travail.

Toutefois, nous pouvons déjà identifier un certain nombre de problèmes potentiels. Premièrement, l'utilisation des ordinateurs portés (à l'image de ceux présentés au début du présent rapport) suscite certaines inquiétudes quant aux effets physiques éventuels d'un usage prolongé. Comme on l'a souligné, un ordinateur courant porté au poignet pèse 320 grammes, et 350 g lorsqu'il est muni d'un radio transmetteur/récepteur. Les appareils de lecture optique portés à l'index pèsent généralement 50 grammes, l'appareil étant déclenché par des pressions régulières du pouce[67].

L'essor mondial du téléphone mobile a suscité certaines inquiétudes quant aux dangers potentiels des radiations électromagnétiques, un domaine de la recherche qui n'a pas abouti pour l'instant à des résultats concluants. Rares sont les travaux effectués quant aux répercussions des autres technologies de surveillance. Quant aux implants de puces RFID, la Federal Drugs Agency des États-Unis a accordé la licence d'exploitation du VeriChip mais a tout de même formulé une liste de risques potentiels pour la santé et notamment: "réactions indésirables des tissus, migration du transpondeur implanté, défectuosité de l'inserter, défectuosité du scanner électronique, interférences électromagnétiques, dangers électriques, incompatibilité avec l'imagerie à résonance magnétique et perçage par aiguille."[68]

De manière générale, le vaste gisement de données fournies par la recherche laisse supposer qu'il existe un lien entre l'instauration de la surveillance du

rendement et l'accroissement des problèmes de santé/sécurité des travailleurs. Le stress est le premier et le plus évident des résultats en ce domaine. Dès 1993, le rapport de l'OIT sur la surveillance électronique au travail évoquait déjà ce problème :

Une étude menée conjointement par des chercheurs de l'Université du Wisconsin et le Communications Workers of America (CVWA) sur la surveillance électronique et le stress au travail confirme les résultats d'études précédentes, laissant supposer que la surveillance électronique est un facteur de stress majeur au travail, notamment en raison du sentiment d'impuissance que ressentent les travailleurs.[69]

Le stress, qui est l'un des principaux sujets de préoccupation dans les centres d'appel, a été examiné lors de la Conférence d'UNI sur les centres d'appel en 2005. Les participants ont préconisé la mise en oeuvre d'une campagne en vue d'améliorer la santé et le bien-être des travailleurs employés dans les centres d'appel, et notamment une action pour réduire le stress, l'anxiété, l'épuisement professionnel et la dépression.

 Chez Verizon South à New Jersey, le rendement des salariés est mesuré sur la base des résultats d'une équipe plutôt que de manière individuelle - une pratique qui a été recommandée par le Comité du CWA-Verizon sur le stress[70].

Depuis quelques années, le stress au travail commence à être réellement reconnu comme un problème de santé et de sécurité au travail. En 2004, les partenaires sociaux européens ont par exemple adopté un accord-cadre sur le stress d'origine professionnelle. Pour autant, les liens entre la surveillance électronique et le stress sont encore mal connus et l'accord-cadre de l'UE par exemple n'évoque pas spécifiquement la relation entre le stress et la surveillance.

Vie privée et travail décent

Le fond du problème que posent le contrôle et la surveillance est celui du droit fondamental des travailleurs à la protection de leur vie privée. Ainsi qu'il ressort d'un rapport de l'UE: "Les salariés n'abandonnent pas leur droit à la vie privée et à la protection des données chaque matin, en franchissant le seuil de leur lieu de travail"[71]. De fait, le droit à la vie privée devient d'autant plus important que la ligne de démarcation entre la vie professionnelle et la vie privée s'estompe progressivement, notamment en raison du développement du télétravail et des contrats d'horaires flexibles.

Il y a bientôt dix ans que l'OIT s'efforce de résoudre les problèmes d'atteinte à la vie privée liés au stockage des données à caractère personnel. Son recueil de directives pratiques (facultatives) sur la protection des données personnelles des travailleurs inclut une brève disposition sur la surveillance[72].

 La section 6.14 du Recueil de l'OIT dispose que:
Dans le cas où les travailleurs font l'objet d'une surveillance, ils devraient être informés à l'avance des raisons de cette surveillance, des périodes concernées, des méthodes et techniques utilisées, ainsi que des données collectées. L'employeur doit réduire à un minimum l'ingérence dans la vie privée des travailleurs.

Toute surveillance secrète ne saurait être autorisée que:
- si elle est conforme à la législation nationale, ou
- s'il existe des soupçons raisonnablement justifiés d'activités criminelles ou d'autres infractions graves

Toute surveillance permanente ne saurait être autorisée que pour des raisons de santé et de sécurité ou en vue de protéger les biens de l'entreprise.

Depuis lors, les problèmes d'atteinte à la vie privée des travailleurs ont été plutôt traités de manière indirecte par des législations générales sur la protection des données. Dans l'Union européenne, par exemple, les États membres sont tenus d'incorporer à leur législation les prescriptions de la directive de 1995 relative à la protection des données. La Commission européenne a proposé de traiter les questions spécifiques de protection des données au travail dans le cadre du dialogue social entre les partenaires sociaux. En 2002, la Commission a élaboré une proposition détaillée d'accord-cadre (voir ci-dessous) destiné à être utilisé dans ces délibérations. Toutefois, le rapport de suivi de la Commission, dont la diffusion était prévue en 2004, n'a pas été publié et le problème semble maintenant avoir été discrètement remisé sur une "voie de garage".

 Le projet d'accord-cadre européen énonce une série de principes, dont le droit des représentants des travailleurs d'être informés et consultés avant la mise en vigueur ou la modification des mesures de contrôle/surveillance, des dispositions restrictives sur la surveillance permanente, des directives strictes sur la surveillance secrète et l'interdiction de la surveillance régulière du courrier électronique et de l'Internet. Il énonce en outre que "l'évaluation des performances des travailleurs et la prise de décision à leur égard ne devrait pas être fondée exclusivement sur des données à caractère personnel collectées dans le cadre d'une surveillance électronique"[73].

Nous avons aussi un bon exemple de législation utile avec la Loi sur la surveillance au travail adoptée en Nouvelles Galles du Sud, (Australie) par le gouvernement travailliste de cet État en 2005. Cette loi étend les contrôles initialement prévus dans la Loi de 1998 sur la vidéosurveillance dans le travail à

d'autres formes nouvelles de surveillance électronique. Aux États-Unis, le CWA (Communications Workers of America) a élaboré un projet de loi semblable visant à restreindre le recours à la vidéosurveillance et aux écoutes sur le lieu de travail - loi qui doit encore être adoptée par le Congrès[74].

Un certain nombre de fédérations syndicales et syndicats individuels ont établi des codes de bonne conduite quant à la protection de la vie privée des travailleurs. Il en existe un exemple aux Pays-Bas, où le FNV a élaboré un règlement modèle sur la vie privée[75]. L'Association des professionnels de TI (qui fait partie du syndicat anglo-irlandais Amicus) a elle aussi élaboré un projet analogue de code de pratique[76].

De telles initiatives concourent à démontrer que la collecte de données électroniques sur les travailleurs par diverses formes de surveillance patronale n'est pas un simple problème technique de respect des normes de protection des données. Ce qui est en question ici, ce sont les droits humains fondamentaux et au final, la dignité humaine.

Conclusion: la voie à suivre pour UNI

Même si la surveillance et le contrôle électroniques s'intensifient dans de nombreux secteurs, il ne s'agit pas de tomber dans un pessimisme résigné face aux technologies. Il existe déjà une multitude d'exemples de bonnes pratiques adoptées par les syndicats et d'autres organisations pour réagir à cette évolution. Après le succès de l'initiative sur les droits en ligne pour les travailleurs en ligne et celui de la campagne sur le travail dans les centres d'appels, y compris la récente Conférence mondiale sur les centres d'appels, UNI détient déjà une solide expérience en ce domaine. Les affiliés d'UNI et d'autres organisations syndicales ont eux aussi remporté des succès (dont certains sont évoqués dans le présent rapport) et qui méritent d'être partagés.

Néanmoins, il convient qu'UNI réfléchisse aux moyens d'intensifier au maximum son action sur le contrôle et la surveillance électroniques. Elle pourrait en particulier envisager un certain nombre de nouvelles mesures.

1 L'évolution ultrarapide de la technologie RFID s'est faite de manière très discrète. La surveillance au moyen de la technologie RFID devient de plus en plus banale, en particulier pour les badges nominatifs munis d'une puce RFID portés par les salariés. L'UNI publiera un Code de bonnes pratiques (comparable à son excellent Code sur les droits en ligne) afin de faciliter le travail des affiliés.

2 La surveillance au moyen de la puce RFID renvoie également à des questions plus générales de surveillance des travailleurs à l'aide du GPS et du téléphone mobile. L'UNI lancera une vaste campagne mondiale ("*Qui surveille vos déplacements ?*") afin d'aider les affiliés et leurs adhérents à mieux comprendre et traiter ces problèmes. Le rapport sera soumis au débat dans chacun des syndicats mondiaux d'UNI.

3 L'OIT sera incitée à se pencher sur les questions de surveillance et de contrôle électroniques. Les travaux de recherche approfondis entrepris par l'OIT en ce domaine remontent à plus de dix ans. Le thème du contrôle et de la surveillance électroniques peut être considéré comme étant en corrélation directe avec l'appel de l'OIT en faveur du travail décent.

4 L'UNI engagera une coopération avec l'Union européenne et d'autres organisations régionales sur ces questions, et participera à la consultation en cours de la Commission européenne sur la technologie RFID.

5 L'UNI s'appuiera sur son site Internet pour donner une large diffusion aux effets d'une surveillance excessive sur la santé et la sécurité.

6 L'UNI continuera de promouvoir vigoureusement la Charte sur les centres d'appels et le Code de pratique sur les droits en ligne.

7 Le contrôle et la surveillance électroniques ne sont pas des caractéristiques visant exclusivement le lieu de travail. Les affiliés d'UNI sont invités à faire cause commune avec les organisations qui oeuvrent pour les libertés civiles et la défense de la vie privée, et à participer à des campagnes plus vastes concernant la manière dont les nouvelles technologies sont instituées (par exemple la campagne menée par les consommateurs des États-Unis contre l'usage de la RFID pour surveiller la clientèle).

Notes

[1] Ce récit s'appuie sur des événements et des problèmes réels
[2] http://www.nocards.org, http://www.spychips.com
[3] Alorie Gilbert, Elementary school nixes electronic ID, February 17 2005 http://news.com.com/2102-1029_3-5581275.html
[4] Andrew Bibby, Invasion of the privacy snatchers, Financial Times, January 9 2006
[5] Paul Tyrrell, Tuned in to the right frequency, Financial Times, December 15 2004
[6] Posting on Smart Mobs, http://www.smartmobs.com/archive/2005/05/04/rfid_employee_m.html. See also http://ubiks.net/local/blog/jmt/archives3/003741.html
[7] from http://www.spychips.com
[8] Will Sturgeon, Las Vegas casino goes for RFID, April 15 2005 http://software.silicon.com/security/0,39024888,39129583,00.htm
[9] Accenture, Silent Commerce Chips Away at Star City Casino Wardrobe Worries, case study, http://www.accenture.com/Global/Services/By_Subject/Radio_Frequency_Identification/Client_Successes/StarCityCasino.htm
[10] WaspTime see http://www.waspbarcode.com/wasptime/wasptime_premium.asp
[11] RAseND, Research brief, Privacy in the Workplace, 2005. See also RAND, Technical Report, 9 to 5: Do you know if your boss knows where you are? 2005 http://www.rand.org
[12] Résolution sur l'identification par radio-fréquence, 20 November 2003
[13] Groupe de travail Article 29 sur la protection des données, document de travail sur les questions de protection des données liées à la RFID, 19 janvier 2005, WP105
[14] GMB Press release, GMB seeks changes to European law to outlaw worker tagging, July 18 2005 http://www.gmb.org.uk/Templates/Internal.asp?NodeID=92057
[15] Cornelia Brandt, Klüger als die intelligenten Dinge sein… Risikoabschätzung bei RFID-Anwendung fordert Handeln auf verschiedenen Ebenen, 2005
[16] UNI Commerce, Technology and RFID must be negotiated January 26 2005 http://www.union-network.org/UNIsite/Sectors/Commerce/Social%20dialogue%20articles/EU_dialogue_increasingly_important.htm
[17] GMB Press release, GMB Congress demands to electronic tagging of workers 'battery farm; workplaces, June 6 2005 http://www.gmb.org.uk/Templates/Internal.asp?NodeID=91861
[18] http://www.peaktech.com/html/products/barcode_scanner/wearable.htm
[19] Case study, Hands-free Plus real-time, equals business advantage, http://www.symbol.com/category.php?fileName=CS-27_Peacocks.xml
[20] Voir par exemple Katrina Arabe, Wearable Computers: the new warehouse wear, 13 février 2003, http://news.thomasnet.com/IMT/archives/2003/02/wearable_comput.html
[21] Michael Blakemore, I-DRA Ltd/GMB, Surveillance in the Workplace – an overview of issues of privacy, monitoring and ethics, September 2005
[22] Eurotechnology Japan, Location Based Mobile Services in Japan, http://www.gii.co.jp/english/ek32275-mobile-services.html
[23] National Workrights Institute, Privacy Under Siege: Electronic Monitoring in the Workplace, n.d.
[24] Adam Geller, Bosses keep sharp eye on mobile workers via GPS, Associated Press, January 3 2005 http://www.workrights.org/in_the_news/in_the_news_associatedpress.html
[25] On Board Computer – Big Brother Comes to CPC
[26] Accord entre Postes Canada et le Syndicat canadien des travailleurs et travailleuses des postes STTP (expiration au 31 janvier 2007)
[27] National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace n.d.; Gundars Kaupins and Robert Minch, Legal and Ethical Implications of Employee Location Monitoring, Proceedings of the 38th Hawaii International Conference on System Sciences
[28] David Hencke, AA to log cal centre staff's trips to loo in pay deal, The Guardian, October 31 2005
[29] American Management Association, 2005 Electronic Monitoring and Surveillance Survey
[30] See for example Jonathan Raper, Technology Trends- brave new world?, http://www.geoplace.com/ge/2001/0101/0101tt.asp
[31] David Canton, Employee Tracking and Monitoring, http://www.canton.elegal.ca/archives/2005/06/. Another checklist for employers is offered by

Gundars Kaupins and Robert Minch, Legal and Ethical Implications of Employee Location Monitoring.
[32] National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace n.d
[33] Hazards magazine, Stop Snooping, http://www.hazards.org/privacy/
[34] For example at Guy's Hospital, London. Hazards magazine, Stop Snooping, http://www.hazards.org/privacy/
[35] Gregor Wittich, Rechtsprechungsübersicht zur Verwendung neue Medien im Betrieb, in DGB, Internet und E-Mail: Neue Medien im Betrieb, 2004
[36] Groupe de travail Article 29 sur la protection des données, Avis 4/2004 sur le traitement des données à caractère personnel au moyen de la vidéo-surveillance, adopté le 11 février 2004. Voir aussi Groupe de travail Article 29 sur la protection des données à caractère personnel au moyen de la vidéosurveillance, adopté le 25 novembre 2002.
[37] Anthony Hildebrand, Branching Out, http://www.smtdirect.co.uk/story.asp ?sectioncode=0&storyCode=3060661
[38] Information du syndicat, janvier 2006
[39] Prof Frank Hendrickx, Protection of workers' personal data in the European Union, Study 2: surveillance and monitoring at work
[40] FGTB, Surveillance par caméras: la CCT no 68, http://www.fgtb.be/code/fr/Documents/2003/ViePrivee/c15_03e0404.htm
[41] http://www.union-network.org/UNIsite/Sectors/IBITS/ICT/online.htm
[42] FNV Bondgenoten, Model Protocol: privacy in the use of the internet and e-mail, n.d.
[43] Cornelia Brandt, Onlinerechte für Beschäftigte, in DGB, Internet und E-mail: Neue Medien im Betrieb, September 2004
[44] Eckpunkte der Nutzung von Internet, Intranet und E-mail im Arbeitsverhältnis, in DGB, Internet und E-mail: Neue Medien im Betrieb, September 2004
[45] Observatoire européen des relations industrielles, New technology and respect for privacy at the workplace, 2003 http://www.eiro.eurofound.eu.int
[46] http://www.fgtb.be/code/fr/Documents/2003/ViePrivee/c15_03e0405.htm
[47] Groupe de travail Article 29 sur la protection des données, document de travail sur la surveillance des communications électroniques sur le lieu de travail, adopté le 29 mai 2002, WP55
[48] Commission européenne, Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs 2002 http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultationdataprot_en.pdf
[49] Professor Vincent Mosco, What are Workers Doing about electronic surveillance in the workplace? An examination of trade union agreements in Canada, proposal for presentation at the 2005 Conference of IFIP Working Group 9-2 Conference
[50] American Management Association, 2005 Electronic Monitoring and Surveillance Survey
[51] Hubert Bouchet, La cybersurveillance sur les lieux de travail, CNIL March 2004
[52] Michael Sommer, Cornelia Brandt and Lothan Schröder (eds), Im Netz@work, VSA-Verlag, 2003
[53] American Management Association, 2005 Electronic Monitoring and Surveillance Survey
[54] Andrew Bibby, Syndicalisation dans les centres d'appel du secteur financier, UNI, 2000
[55] UNI Global Call Centre News, avril 2004
[56] Communications Workers of America, http://www.cwa-union.org/workers/customer/protections.asp
[57] Philip Taylor and Peter Bain, Trade Unions and Call Centre Survey, for Finance Sector Unions, 2000
[58] Hazards magazine, Stop Snooping, http://www.hazards.org/privacy/
[59] http://www.cupw.ca/pages/document_eng.php?Doc_ID=595
[60] Photo from http://www.spychips.com
[61] Michael Blakemore, Every breath you take, every move you make, http://www.unionweb.co.uk/view/PageView.aspx?Page=273

[62] Martin Dodge, Rob Kitchin, The ethics of forgetting in an age of pervasive computing, UCL, http://www.casa.icl.ac.uk. A Galloway, Intimations of everyday life: ubiquitous computing and the city, Cultural studies, 18 (2/3), 2004
[63] OIT, Conditions of work digest volume 12: Workers' privacy: Part II, monitoring and surveillance in the workplace, 1993
[64] Gary Marx, Measuring Everything that Moves: the new surveillance at work, in I and R Simpson, The Workplace and Deviance, 1999, http://web.mit.edu/gtmarx/www/ida6.html
[65] How Wal-Mart keeps Unions At Bay, Business Week, October 28 2002 http://72.14.207.104/search?q=cache:YRWfcqtIO2IJ:www.2110uaw.org/gseu/archive/How%2520WalMart%2520Keeps%2520Unions%2520at%2520Bay.htm+surveillance+cameras+workplace+union+organizing+drive&hl=en&gl=uk&ct=clnk&cd=2
[66] Eric Lee, Trade Unions in the electronic workplace, April 13 2004 http://www.ericless.me.uk/archive/000079.html
[67] http://www.peaktech.com/html/products/barcode_scanner/wearable.htm
[68] http://www.sec.gov/Archives/edgar/data/924642/000106880004000587/ex99p2.txt
[69] OIT, Conditions of work digest volume 12: Workers' privacy: Part II, monitoring and surveillance in the workplace, 1993
[70] Communications Workers of America, http://www.cwa-union.org/workers/customer/protections.asp
[71]Groupe de travail Article 29 sur la protection des données, document sur la surveillance des communications électroniques sur le lieu de travail, adopté le 29 mai 2002, WP55
[72] OIT, Recueil Protection des données personnelles des travailleurs, 1997 http://www.ilo.org/public/english/protection/safework/cops/french/download/f000011.pdf
[73] Commission européenne, Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs, http://ec.europa.eu/employment_social/news/2002/oct/data_prot_fr.pdf
[74] CWA-Backed bill would protect workers' privacy in changing areas, CWA press release, March 1 2005. http://www.cwa-union.org/news/cwa-news/page.jsp?itemID=27374804
[75]http://home.fnv.nl/02werkgeld/arbo/wetgeving/privacy/Model%20Privacyreglement/model_privacyreglement1.htm
[76] http://www.amicus-itpa.org/juneconf2.shtml